

09/290 363

WEST

☐ Generate Collection☐ Print

L4: Entry 1 of 7

File: USPT

Jun 26, 2001

US-PAT-NO: 6253193

DOCUMENT-IDENTIFIER: US 6253193 B1

\*\* See image for Certificate of Correction \*\*

TITLE: Systems and methods for the secure transaction management and electronic rights protection

DATE-ISSUED: June 26, 2001

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/57; 705/52

ABSTRACT: ✓

✓ The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

72 Claims, 155 Drawing figures  
Exemplary Claim Number: 1  
Number of Drawing Sheets: 146



Generate Collection

Print

L4: Entry 2 of 7

File: USPT

Nov 9, 1999

US-PAT-NO: 5982891

DOCUMENT-IDENTIFIER: US 5982891 A

8/964338 c1

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: November 9, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/54; 705/26, 713/167

## ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

102 Claims, 153 Drawing figures

Exemplary Claim Number: 1

Number of Drawing Sheets: 146



Generate Collection

Print

4

L4: Entry 3 of 7

File: USPT

Sep 7, 1999

US-PAT-NO: 5949876

DOCUMENT-IDENTIFIER: US 5949876 A

8/778256

\*\* See image for Certificate of Correction \*\*

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: September 7, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/80; 705/1, 705/39, 705/54

## ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

375 Claims, 155 Drawing figures  
Exemplary Claim Number: 1  
Number of Drawing Sheets: 146



Generate Collection

Print

L4: Entry 4 of 7

File: USPT

Jun 29, 1999

US-PAT-NO: 5917912

DOCUMENT-IDENTIFIER: US 5917912 A

8/780545

TITLE: System and methods for secure transaction management and electronic rights protection

DATE-ISSUED: June 29, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 713/187; 705/40, 709/312, 713/164

## ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

58 Claims, 153 Drawing figures  
Exemplary Claim Number: 58  
Number of Drawing Sheets: 146



Generate Collection

Print

L4: Entry 5 of 7

File: USPT

Y ?  
Jun 22, 1999

US-PAT-NO: 5915019

DOCUMENT-IDENTIFIER: US 5915019 A 8/780393

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: June 22, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/54; 705/26, 705/400, 713/200

## ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

101 Claims, 155 Drawing figures  
Exemplary Claim Number: 1  
Number of Drawing Sheets: 146



Generate Collection

Print

L4: Entry 6 of 7

File: USPT

Jun 8, 1999

US-PAT-NO: 5910987

DOCUMENT-IDENTIFIER: US 5910987 A

8/760440

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: June 8, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/52; 705/30

## ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

2 Claims, 155 Drawing figures

Exemplary Claim Number: 1

Number of Drawing Sheets: 146

## End of Result Set



Generate Collection

Print

L4: Entry 7 of 7

File: USPT

Apr 6, 1999

US-PAT-NO: 5892900

DOCUMENT-IDENTIFIER: US 5892900 A 8/706206

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: April 6, 1999

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Sibert; W. Olin	Lexington	MA		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 713/200; 713/201

## ABSTRACT:

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway."

220 Claims, 177 Drawing figures

Exemplary Claim Number: 1

Number of Drawing Sheets: 163

9/290363

## WEST Search History

DATE: Wednesday, April 30, 2003

Set Name Query  
side by sideHit Count Set Name  
result set

DB=JPAB,EPAB,DWPI; THES=ASSIGNEE; PLUR=YES; OP=OR

L11 L10 and @pd&lt;=19990326

0 L11

L10 (drm or (digital\$ adj right\$ adj manag\$)) and (decrypt\$ or encrypt\$ or crypto\$) and (digital\$ with licens\$)

10 L10

L9 (drm or (digital\$ adj right\$ adj manag\$)) and ((black adj box) or blackbox or "black-box") and (digital\$ with licens\$)

1 L9

DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR

L8 (drm or (digital\$ adj right\$ adj manag\$)) and (((black adj box) or blackbox or "black-box") same (decrypt\$ or encrypt\$ or crypto\$)) and (digital\$ with licens\$) and @ad&lt;=19990326

7 L8

L7 (drm or (digital\$ adj right\$ adj manag\$)) and ((black adj box) or blackbox or "black-box").ab. and (digital\$ with licens\$) and @ad&lt;=19990326

0 L7

L6 (drm or (digital\$ adj right\$ adj manag\$)) and ((black adj box) or blackbox or "black-box").clm. and (digital\$ with licens\$) and @ad&lt;=19990326

0 L6

L5 (drm or (digital\$ adj right\$ adj manag\$)) and (((black adj box) or blackbox or "black-box") and (digital\$ with licens\$)).clm. and @ad&lt;=19990326

0 L5

L4 L3 and (encrypt\$ or decrypt\$ or crypto\$)

7 L4

L3 l1 and @ad&lt;=19990326

7 L3

DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE;  
PLUR=YES; OP=OR

L2 l1 and @pd&lt;=19990326

0 L2

L1 (drm or (digital\$ adj right\$ adj manag\$)) and ((black adj box) or blackbox or "black-box") and (digital\$ with licens\$)

24 L1

END OF SEARCH HISTORY





Generate Collection

Print

L8: Entry 1 of 7

File: USPT

Jun 26, 2001

DOCUMENT-IDENTIFIER: US 6253193 B1

\*\* See image for Certificate of Correction \*\*

TITLE: Systems and methods for the secure transaction management and electronic rights protection

Application Filing Date (1):  
19981209Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1587):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1764):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit

information contained is securely processed at said clearinghouse VDE node by said inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box" that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (79):

Robert Weber, Document from the Internet: Digital Rights Management Technologies, Oct. 1995, 21 pages.

Other Reference Publication (80):

Robert Weber, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Northeast Consulting Resources, Inc., Oct. 1995, 49 pages.



Generate Collection

Print

L8: Entry 2 of 7

File: USPT

Nov 9, 1999

DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):  
19971104Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1575):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1759):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said

inverse (return) ~~audit~~ method, the clearinghouse V node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box" that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (124):

Document from Internet, "Digital Rights Management Technologies," Robert Weber, 21 pages (Oct. 1995).

Other Reference Publication (125):

Weber, Robert, "Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations," Northeast Consulting Resources, Inc., 49 pages (Oct. 1995).



Generate Collection

Print

L8: Entry 3 of 7

File: USPT

Sep 7, 1999

DOCUMENT-IDENTIFIER: US 5949876 A

**\*\* See image for Certificate of Correction \*\***

TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):  
19970108Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1577):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1754):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit

information contained is securely processed at said clearinghouse VDE node by said inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box" that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (68):

Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.

Other Reference Publication (69):

Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.



Generate Collection

Print

L8: Entry 4 of 7

File: USPT

Jun 29, 1999

DOCUMENT-IDENTIFIER: US 5917912 A

TITLE: System and methods for secure transaction management and electronic rights protection

Application Filing Date (1):

19970108

Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1566):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1742):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said

inverse (return) audit method, the clearinghouse V node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE 650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (57):

Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.

Other Reference Publication (58):

Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.





Generate Collection

Print

L8: Entry 5 of 7

File: USPT

Jun 22, 1999

DOCUMENT-IDENTIFIER: US 5915019 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):  
19970108Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1572):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1757):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said

inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (48):

Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.

Other Reference Publication (49):

Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.



Generate Collection

Print

L8: Entry 6 of 7

File: USPT

Jun 8, 1999

DOCUMENT-IDENTIFIER: US 5910987 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):  
19961204

Brief Summary Text (143):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1573):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1751):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said

inverse (return) audit method, the clearinghouse V node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (58):

Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.

Other Reference Publication (59):

Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.

End of Result Set



Generate Collection

Print

L8: Entry 7 of 7

File: USPT

Apr 6, 1999

DOCUMENT-IDENTIFIER: US 5892900 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):  
19960830Brief Summary Text (142):

VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. VDE further includes highly configurable transaction operating system technology, one or more associated libraries of load modules along with affiliated data, VDE related administration, data preparation, and analysis applications, as well as system software designed to enable VDE integration into host environments and applications. VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques.

Detailed Description Text (1798):

An electronic contract is an electronic form of an agreement including rights, restrictions, and obligations of the parties to the agreement. In many cases, electronic agreements may surround the use of digitally provided content; for example, a license to view a digitally distributed movie. It is not required, however, that an electronic agreement be conditioned on the presence or use of electronic content by one or more parties to the agreement. In its simplest form, an electronic agreement contains a right and a control that governs how that right is used.

Detailed Description Text (1975):

Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit

information contained is securely processed at said clearinghouse VDE node by said inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

Other Reference Publication (129):

Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.

Other Reference Publication (130):

Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.

## End of Result Set



Generate Collection

Print

A

L9: Entry 1 of 1

File: DWPI

Jul 19, 2001

DERWENT-ACC-NO: 2001-496746  
 DERWENT-WEEK: 200154  
 COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital rights management system operating on computing device when user requests an encrypted digital content to be rendered by the computer

INVENTOR: GANESAN, K; LIU, D ; PEINADO, M

PATENT-ASSIGNEE: MICROSOFT CORP (MICT)

PRIORITY-DATA: 2000US-0526290 (March 15, 2000), 2000US-176425P (January 14, 2000)

## PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200152021 A1	July 19, 2001	E	126	G06F001/00
AU 200069281 A	July 24, 2001		000	G06F001/00

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ  
 EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD  
 MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU  
 ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD  
 SE SL SZ TZ UG ZW

## APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200152021A1	August 22, 2000	2000WO-US23108	
AU 200069281A	August 22, 2000	2000AU-0069281	
AU 200069281A		WO 200152021	Based on

INT-CL (IPC): G06 F 1/00

RELATED-ACC-NO: 2001-522158;2001-522159 ;2001-596328 ;2001-596397

ABSTRACTED-PUB-NO: WO 200152021A

## BASIC-ABSTRACT:

NOVELTY - Uses a black box (30) in the digital rights management (DRM) system for performing decryption and encryption functions. The black box contains identifier of computing device (14) and is tied to the computing device.

DETAILED DESCRIPTION - The black box also contains at least one black box public key. The DRM system also contains digital license (16) corresponding to the digital content. The licence includes a decryption key (KD) for decrypting the encrypted digital content. The decryption key is encrypted according to a black box public key of the black box. The licence is tied to the black box, and the computing device. AN INDEPENDENT CLAIM is made for a method of operating DRM system when user requests that computer renders an encrypted digital content.

USE - For enforcing rights in a digital content allowing access to encrypted digital content only in accordance with parameters specified by licence rights acquired by user.

ADVANTAGE - Enforcement rights and method enforce rights in protected (secure) digital content available on a medium such as the Internet, an optical disk, etc.

DESCRIPTION OF DRAWING(S) - Drawing is a block diagram showing an enforcement architecture in accordance with an embodiment of the present invention.

Computing device 14

Digital licence 16

Black box 30

Decryption key. KD

ABSTRACTED-PUB-NO: WO 200152021A  
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/22

DERWENT-CLASS: T01  
EPI-CODES: T01-C01A; T01-D01; T01-H01B1; T01-H01C2; T01-H07C5E; T01-J12C;  
T01-J20B2A;



☐ Generate Collection

☐ Print

A L10: Entry 1 of 10

File: DWPI

Dec 26, 2002

DERWENT-ACC-NO: 2003-094046  
 DERWENT-WEEK: 200315  
 COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Duplicating secure digital music by generating licensing data in accordance with digital rights management level for content files and encrypting

INVENTOR: ISAACSON, S R; PETERS, E R ; SHORT, R L

PATENT-ASSIGNEE: IOMEGA CORP (IOMEN)

PRIORITY-DATA: 2001US-0891441 (June 25, 2001)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 20020196940 A1	December 26, 2002		000	H04L009/00
WO 2003001352 A2	January 3, 2003	E	035	G06F001/00

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
US20020196940A1	June 25, 2001	2001US-0891441	
WO2003001352A2	June 21, 2002	2002WO-US19989	

INT-CL (IPC): G06 F 1/00; H04 L 9/00

ABSTRACTED-PUB-NO: WO2003001352A  
 BASIC-ABSTRACT:

NOVELTY - Method consists in copying self-authenticating digital data and associated licensing data representing licensing rights from a master storage medium to a target storage medium (TSM), integrating the TSM serial number information. Licensing data is WMA formatted, content files are selected for duplication, digital rights management (DRM) levels are set for the content files and the licensing data is generated in accordance with the DRM rights level. The file is encrypted with a unique key stored in the file and its licensing data.

DETAILED DESCRIPTION - There are INDEPENDENT CLAIMS for:

- (1) A computer program for duplicating secure digital data
- (2) A computer system with master storage medium copying to target storage media

USE - Method is for providing secure digital music duplication.

DESCRIPTION OF DRAWING(S) - The figure shows a system for producing a benchmark on storage media.

ABSTRACTED-PUB-NO 02003001352A  
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/10

DERWENT-CLASS: T01  
EPI-CODES: T01-D01; T01-J20B2A; T01-S03;



Generate Collection

Print

L10: Entry 2 of 10

File: DWPI

Dec 3, 2002

A  
 DERWENT-ACC-NO: 2003-041103  
 DERWENT-WEEK: 200304  
 COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Applet execution method for software license protection in multi-processor computer environment, involves determining whether applet has right to be executed, using sequence data stored in tamper-resistant device

INVENTOR: CARLSEN, U; HAMMERSTAD, H

PATENT-ASSIGNEE: SOSPITA AS (SOSPN)

PRIORITY-DATA: 2001WO-NO00201 (May 11, 2001)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 6490720 B1	December 3, 2002		000	G06F009/44
WO 200293365 A1	November 21, 2002	E	017	G06F009/44

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
US 6490720B1	May 11, 2001	2001WO-NO00201	Cont of
US 6490720B1	June 26, 2001	2001US-0891490	
WO 200293365A1	May 11, 2001	2001WO-NO00201	

INT-CL (IPC): G06 F 9/44; G06 F 9/46

ABSTRACTED-PUB-NO: WO 200293365A

BASIC-ABSTRACT:

NOVELTY - A portion of a code, having several applets, is executed in one or more tamper-resistant devices (200) such as smart cards which are connected to a computer (100). A sequence data stored in the tamper-resistant device is used to determine whether the applet has the right to be executed, when the sequence data exist in the current applet.

USE - For executing applets in tamper-resistant external devices such as smart cards, USB tokens, PCMCIA cards and micro controllers for software license protection in applications, such as e-payment, digital rights management (DRM), multimedia protection, authentication, biometry, public-key infrastructure (PKI) and encryption-schemes, in multi-processor computer environment.

ADVANTAGE - Allows a smart card application to be safely split up into sub applications, thereby enforcing correct execution order and application integrity and allowing the execution environment of the external device to discover illegal processing of the applets. Provides an efficient and user-friendly tool for optimization of application security and performance by selecting software

application components that are suitable and not suitable for execution in the tamper-resistant device.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the multi-processor computer environment for executing a portion of code in an external device.

Computer 100

Tamper-resistant device 200

ABSTRACTED-PUB-NO: WO 200293365A  
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.3/5

DERWENT-CLASS: T01  
EPI-CODES: T01-C11; T01-F03; T01-H01B3A; T01-J20B2A;



Generate Collection

Print

L10: Entry 4 of 10

File: DWPI

Dec 27, 2001

DERWENT-ACC-NO: 2002-257107  
 DERWENT-WEEK: 200230  
 COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Content distribution system via network utilizing distribution conditional access agents and secure agents to perform digital rights management in a secure environment

INVENTOR: FRANS DONK, R W

PATENT-ASSIGNEE: MINDPORT USA (MINDN)

PRIORITY-DATA: 2000US-212125P (June 16, 2000)

## PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200198903 A1	December 27, 2001	E	114	G06F011/30
AU 200169856 A	January 2, 2002		000	G06F011/30

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

## APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200198903A1	June 15, 2001	2001WO-US19271	
AU 200169856A	June 15, 2001	2001AU-0069856	
AU 200169856A		WO 200198903	Based on

INT-CL (IPC): G06 F 11/30; G06 F 12/14; G06 F 15/16; G06 F 15/173; G06 F 17/60; H04 K 1/00; H04 L 9/00; H04 L 9/32

ABSTRACTED-PUB-NO: WO 200198903A  
 BASIC-ABSTRACT:

NOVELTY - Clear content (24) at the content provider (16) is encrypted utilizing a symmetric product key to generate encrypted content (26), which is communicated via a network (18) to a content distributor (20). A conditional access agent (28) may decrypt the encrypted content to regenerate the clear content in a secure environment and watermarks the content for delivery to a specific content destination (22). The watermarked content (30) can be distributed to a conditional access client (32) or the access agent may re-encrypt the content with a public key.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method to distribute content via a network, for a method and system to provide an encryption key storage and distribution service, for a method and system of securing content for distribution and for methods to digitally sign a content license associated with content and to dynamically present a payment gateway to content requesters.

USE - Distributing content via a network.

DESCRIPTION OF DRAWING(S) - The drawing shows the system

Clear content 24

Content provider 16

Encrypted content 26

Content distributor 20

Access agent 28

Destination 22

Access client 32

ABSTRACTED-PUB-NO: WO 200198903A

EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/27

DERWENT-CLASS: T01 W01

EPI-CODES: T01-D01; T01-N01A2A; T01-N01D; T01-N02B1; W01-A05A;

## End of Result Set



Generate Collection

Print

Self L10: Entry 10 of 10

File: DWPI

Mar 5, 2003

DERWENT-ACC-NO: 2000-647267  
 DERWENT-WEEK: 200319  
 COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Enforcement architecture for digital rights management, determines whether right to render digital content in manner sought exists based on digital license stored in computing device

INVENTOR: ABBURI, R; BELL, J R C ; BLINN, A N ; ENGLAND, P ; JAKUBOWSKI, M H ; JONES, T C ; MANFERDELLI, J L ; PEINADO, M ; VENKATESAN, R ; YU, H Y V

PATENT-ASSIGNEE: MICROSOFT CORP (MICT)

PRIORITY-DATA: 1999US-0290363 (April 12, 1999), 1999US-126614P (March 27, 1999)

## PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 1287636 A2	March 5, 2003	E	000	H04L009/00
WO 200059150 A2	October 5, 2000	E	090	H04L009/00
AU 200035039 A	October 16, 2000		000	H04L009/00

DESIGNATED-STATES: AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE AE AL AM  
 AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID  
 IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO  
 RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI  
 FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

## APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
EP 1287636A2	February 25, 2000	2000EP-0913629	
EP 1287636A2	February 25, 2000	2000WO-US04947	
EP 1287636A2		WO 200059150	Based on
WO 200059150A2	February 25, 2000	2000WO-US04947	
AU 200035039A	February 25, 2000	2000AU-0035039	
AU 200035039A		WO 200059150	Based on

INT-CL (IPC): H04 L 9/00

RELATED-ACC-NO: 2000-611744;2000-647268 ;2001-090815 ;2001-191170 ;2001-210824  
 ;2001-210825 ;2002-279866 ;2002-350656 ;2002-392575

ABSTRACTED-PUB-NO: WO 200059150A  
 BASIC-ABSTRACT:

NOVELTY - A computing device (14) receives distributed digital content from a content server (22) and stores digital license corresponding to the digital content (12). A digital rights management (DRM) system on the computing device is invoked by a rendering application and determines whether a right to render digital content in the manner sought exists based on digital license stored in the computing device.

DETAILED DESCRIPTION - The digital content (12) in encrypted form is distributed by

content server and a license server (24) issues digital license corresponding to the digital content. The content and license servers are communicatively coupled to internet. The digital license includes a decryption key for decrypting the encrypted digital content and a description of rights conferred by the license. An INDEPENDENT CLAIM is also included for digital rights management implementing method.

USE - For allowing access to digital contents such as digital audio, video, text and digital multimedia and enforcing rights in protected digital content on a medium such as internet, optical disk. For handheld devices, multiprocessor systems, microprocessor based or programmable consumer electronics, network PCs, mini computers, main frame computers.

ADVANTAGE - Prevents user of the computing device from making a copy of digital content, except otherwise allowed by content owner. Enables user to obtain license from a license server without any action necessary on the part of the user.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of enforcement architecture.

Digital content 12

Computing device 14

Servers 22,24

ABSTRACTED-PUB-NO: WO 200059150A  
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/12

DERWENT-CLASS: W01  
EPI-CODES: W01-A05; W01-A05A;



Generate Collection

Print

## Search Results - Record(s) 1 through 10 of 10 returned.

☐ 1. Document ID: US 20020196940 A1 WO 2003001352 A2

L10: Entry 1 of 10

File: DWPI

Dec 26, 2002

DERWENT-ACC-NO: 2003-094046  
DERWENT-WEEK: 200315  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Duplicating secure digital music by generating licensing data in accordance with digital rights management level for content files and encrypting

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	KWIC
Draw Desc	Clip Img	Image									

☐ 2. Document ID: US 6490720 B1 WO 200293365 A1

L10: Entry 2 of 10

File: DWPI

Dec 3, 2002

DERWENT-ACC-NO: 2003-041103  
DERWENT-WEEK: 200304  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Applet execution method for software license protection in multi-processor computer environment, involves determining whether applet has right to be executed, using sequence data stored in tamper-resistant device

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	KWIC
Draw Desc	Clip Img	Image									

☐ 3. Document ID: EP 1271279 A2 US 20020013772 A1

L10: Entry 3 of 10

File: DWPI

Jan 2, 2003

DERWENT-ACC-NO: 2002-279866  
DERWENT-WEEK: 200310  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital content rendering method for digital right management and enforcement, involves rendering encrypted content on portable device, by decrypting encrypted content key with private key

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	KWIC
Draw Desc	Clip Img	Image								

☐ 4. Document ID: WO 200198903 A1 AU 200169856 A

DERWENT-ACC-NO: 2002-257107  
DERWENT-WEEK: 200230  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Content distribution system via network utilizing distribution conditional access agents and secure agents to perform digital rights management in a secure environment

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWC

☐ 5. Document ID: WO 200152020 A1 AU 200069280 A

L10: Entry 5 of 10

File: DWPI

Jul 19, 2001

DERWENT-ACC-NO: 2001-522159  
DERWENT-WEEK: 200157  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Enforcing rights in digital contents allowing access to encrypted digital content only in accordance with parameters specified by license rights acquired by user

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWC

☐ 6. Document ID: WO 200152021 A1 AU 200069281 A

L10: Entry 6 of 10

File: DWPI

Jul 19, 2001

DERWENT-ACC-NO: 2001-496746  
DERWENT-WEEK: 200154  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital rights management system operating on computing device when user requests an encrypted digital content to be rendered by the computer

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWC

☐ 7. Document ID: EP 1259863 A2 WO 200058811 A2 AU 200037101 A

L10: Entry 7 of 10

File: DWPI

Nov 27, 2002

DERWENT-ACC-NO: 2001-210825  
DERWENT-WEEK: 200302  
COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital rights management system for enforcing rights in digital content, has license evaluator that determines if corresponding stored license enables requesting user to render requested digital content

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWMC

☐ 8. Document ID: WO 200058810 A2 AU 200037087 A

L10: Entry 8 of 10

File: DWPI

Oct 5, 2000

DERWENT-ACC-NO: 2001-210824

DERWENT-WEEK: 200242

COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital content package applicable for access to digital content has license acquisition information including location of digital license provider, and package ID for identifying digital content and package

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWMC

☐ 9. Document ID: WO 200059151 A2 AU 200033810 A

L10: Entry 9 of 10

File: DWPI

Oct 5, 2000

DERWENT-ACC-NO: 2000-647268

DERWENT-WEEK: 200242

COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Digital content in encrypted rights protected form rendering, involves locating digital content of selected license and obtaining decryption key for decrypting digital contents using digital rights management system

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWMC

☐ 10. Document ID: EP 1287636 A2 WO 200059150 A2 AU 200035039 A

L10: Entry 10 of 10

File: DWPI

Mar 5, 2003

DERWENT-ACC-NO: 2000-647267

DERWENT-WEEK: 200319

COPYRIGHT 2003 DERWENT INFORMATION LTD

TITLE: Enforcement architecture for digital rights management, determines whether right to render digital content in manner sought exists based on digital license stored in computing device

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
Draw Desc	Clip Img	Image							

KWMC

Generate Collection

Print

Terms	Documents
(drm or (digital\$ adj right\$ adj manag\$)) and (decrypt\$ or encrypt\$ or crypto\$) and (digital\$ with licens\$)	10

**Display Format:**

[Previous Page](#)

[Next Page](#)